UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC.,

Plaintiff,

v.

Case No.: No. 22-cv-00187

SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1-50,

Defendants.

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S MOTION FOR ADOPTION AND ENTRY OF PROPOSED INSPECTION PROTOCOL

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
Attorneys for Moog Inc.
Rena Andoh
Travis J. Anderson (*pro hac vice*)
Tyler E. Baker (*pro hac vice*)
Kazim A. Naqvi (*pro hac vice*)
30 Rockefeller Plaza
New York, New York 10112
212.653.8700

HODGSON RUSS LLP
Attorneys for Moog Inc.
Robert J. Fluskey, Jr.
Melissa N. Subjeck
Pauline T. Muto
The Guaranty Building
140 Pearl Street, Suite 100
Buffalo, NY 14202-4040
716.856.4000

TABLE OF CONTENTS

Page

Table of Authorities

Page(s)

Cases

I. INTRODUCTION

This case involves both spoliation and theft on a massive scale, including undisputed spoliation of at least 136,994 stolen files from one device, admitted deletion of files on up to dozens more devices, and theft of over 1.3 million files from Moog. The spoliation is so serious that Skyryse's (soon to be former) counsel Gibson Dunn requested an emergency conference with the Court to disclose it. At this conference, Gibson Dunn admitted to the Court that "[w]hat we have seen is – to us, is an alarming series of deletions." (4/26/22 Hrg. Tr. (ECF 95) at 19:4-5).

Nearly all of the evidence of spoliation and theft is on devices belonging to and/or under the sole control of Defendants. Pursuant to the Court's March 11 stipulated temporary restraining order (ECF 25) (the "March 11 Order"), Defendants have to date turned over to a neutral forensic vendor 28 devices precisely because, *in Defendants' own determination*, they contain Moog non-public information. These devices are the heart of this case. Yet Defendants' turnover would be a completely hollow and ineffectual gesture if Moog has no access to these devices to conduct a full and fair investigation. And Moog has, in fact, had zero access—the devices remain a complete black box to Moog—despite the fact that over a month has passed since nearly all the devices were turned over on April 1 (several of the devices were turned over late and in violation of the Court's March 11 Order, on April 29 and May 5). Moog still has no idea exactly what of its data is on the 28 devices. Recently, Skyryse disclosed that an additional 37 devices either contain Moog data or evidence of spoliation, and yet, to the extent Skyryse turns them over to the neutral vendor, they would be destined to also remain in purgatory indefinitely if Skyryse were to have its way.

This case deserves an inspection protocol that permits the full and fair investigation of the "alarming" spoliation and theft that has occurred. Moog's inspection protocol does just this, while simultaneously going above and beyond to address all of the security, confidentiality, privilege, and privacy concerns of the Defendants. *First*, under Moog's protocol, Moog does not get physical

possession of the Defendants' devices or even forensic images of the devices.[1] Instead, that physical possession always stays with the neutral vendor. Moog's outside counsel and experts can only log on to the neutral vendor's computer to review the forensic images, without rights to copy or edit the images. *Second*, this review is monitored (including through videorecording) by the neutral vendor to ensure the security of the data. *Third*, only Moog's outside counsel and experts can review the forensic images, which are by default designated "HIGHLY CONFIDENTIAL—OUTSIDE COUNSEL & EXPERTS' EYES ONLY." While bearing this designation, information from the forensic images cannot be disclosed to in-house counsel or employees of Moog. *Fourth*, before the forensic images are made available for review by Moog's outside counsel and experts, Defendants have an opportunity to review and excise privileged material and, for personal devices, personally private material. Moog's proposed protocol is eminently reasonable.

By contrast, Skyryse's competing protocol seeks to keep the devices shrouded in mystery, in effect erecting a wall between Moog and the evidence of spoliation and theft. Under Skyryse's proposed protocol, Moog gets no access to the forensic images. Instead, Moog can only provide search terms, file names, and hash values to the neutral vendor (that Skyryse must agree to), who then runs those search terms.[2] The neutral vendor then exercises its own "judgment" to determine whether the resulting hits contain Moog data—even though the neutral vendor has no expertise regarding flight control and aviation software development (i.e., the confidential information that

[1] A "forensic image" (sometimes called a "mirror image") of a device is described as a "forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive." *Commc'ns Ctr., Inc. v. Hewitt*, No. 03-cv-1968, 2005 WL 3277983, at *1 (E.D. Cal. Apr. 5, 2005).

[2] A "hash value" is a "unique numeric identifier for [a] digital computer file[]." *United States v. Heleniak*, No. 14-CR-42A, 2015 U.S. Dist. LEXIS 89728, at *3 (W.D.N.Y. July 10, 2015). Where even a single bit or character is changed in a file, the hash value generated from that file will no longer match the original. *See Id.*

was stolen) or Moog's data generally. Skyryse's "inspection" protocol does not contemplate an inspection at all, but is merely a weak echo of the "search" that Skyryse already claims to have conducted in this case, which has proved to be a complete failure and has already resulted in spoliation and violations of the Court's March 11 Order.

Skyryse's protocol would fail in at least the following ways: *First*, searching for words would not fully uncover the extent of the "alarming" spoliation that has occurred. Spoliation means a file has been deleted, resulting in the *absence* of a file and the *absence* of words that were once in that deleted file. *Second*, many of the over 1.3 million files have been stolen (that Moog is currently aware of) are not chiefly composed of human words that can be searched, including drawings, designs, schematics, executables, images, models, diagrams, hand drawn figures, and object files. *Third*, and relatedly, much of the use is not literal copying at all, but adapting Moog's processes, data flows, algorithms, structure, and architecture, where searching for words will be insufficient. *Fourth*, searching for distinctive words is completely ineffectual where these words were deliberately replaced to obfuscate the theft.

Finally, Skyryse's protocol would inject needless and unacceptable delay into this case. Even if mere searching were sufficient here, requiring that it go through a "middle man" like the neutral vendor would play into the very delay strategy that Skyryse has employed from the start. Waiting for Skyryse to approve the search parameters would cause delay. Waiting for the neutral vendor to run the search terms and exercise its "judgment" (uninformed by any aviation expertise) as to whether the resulting files contain Moog data would cause delay. Waiting for Defendants to conduct a privilege review of the files deemed relevant by the neutral vendor would cause delay. And after Moog gets what is left over, reviews those documents, and identifies additional search terms, that process would have to start anew, causing further delay. And this process will repeat,

iteratively, *ad infinitum*. This protracted process is not acceptable, especially as Moog urgently needs relief, including preliminary injunctive relief.

Instead, Skyryse needs to finally make good on its repeated claims of being transparent. (*E.g.,* 4/8/22 Hrg. Tr. (ECF 71) at 14:4-8 ("[W]e're happy to be transparent about what we're doing . . . ."). This means permitting Moog's outside counsel and experts to inspect the forensic images and follow the trail of spoliation, theft, and misappropriation in a full and fair investigation. Notably, the individual Defendants Pilkington and Kim do not object to Moog's proposed protocol. This means of the four parties to this case, only Skyryse maintains an objection to Moog's proposed protocol. Skyryse's objection should be overruled. Moog respectfully requests that the Court adopt and enter its proposed inspection protocol, as well as a schedule to ensure that the forensic images are timely made available for inspection.

II. FACTUAL AND PROCEDURAL BACKGROUND

A. Theft of Moog Data and Spoliation of Evidence

In November 2021, Alin Pilkington, Moog's longtime senior engineer, left Moog to join Skyryse. (Compl. (ECF 1), ¶ 53). Shortly thereafter, on November 19, 2021, Pilkington's direct and close report at Moog, Misook Kim (still employed by Moog at the time), copied 136,994 files from her Moog work computer onto an external hard drive, chiefly comprising Pilkington's work product while at Moog. (Compl., ¶¶ 115, 123; Dec. of Ian Bagnald (ECF 4-18), ¶¶ 8-10). What Kim copied represented over 15 years of Moog's engineering work, including large volumes of source code. (Compl., ¶¶ 117-120; Dec. of Michael Hunter (ECF 4-2), ¶ 63). On December 15, 2021, Kim copied additional Moog data onto this external hard drive. (Compl., ¶ 135; Dec. of Bruce Pixley (ECF 4-28), ¶¶ 25, 33). Two days later, Kim deleted 54 gigabytes of data from her work computer. (Compl., ¶ 135; Pixley Dec., ¶ 27). Shortly thereafter, Kim left Moog to join

Skyryse, taking the external hard drive with her, unbeknownst to Moog. (Compl., ¶¶ 91, 137; Pixley Dec., ¶ 35).

Upon discovering this theft, Moog promptly demanded return of the external hard drive. (Compl., ¶¶ 130-131). In response, Kim returned two external hard drives, both of which contained no files. (Compl., ¶¶ 130-132; Pixley Dec., ¶¶ 28-32). One of the drives, which was the one that received 136,994 Moog files from Kim's work laptop on November 19, 2021, and subsequent Moog data on December 15, 2021, had been intentionally wiped clean and completely spoliated. (*Id*.).

On March 7, 2022, Moog filed this action as well as a motion for preliminary injunction and temporary restraining order. After the filing of this action, Moog discovered further theft, this time directly by Alin Pilkington, namely, that Pilkington had copied over 1.3 million Moog files from his Moog work computer onto an external hard drive, including 130,000 files that were copied on his last day of employment at Moog. (Dec. of Rena Andoh ("Andoh Dec."), Ex. C).

B. Defendants' Stipulated Turnover of Devices Containing Moog Data and Violation of March 11 Order

On March 11, 2022, Defendants stipulated to a temporary restraining order, rather than oppose Moog's motion for same, and the stipulation was entered as a Court order. (ECF 25). In this order, Defendants stipulated to, among other things, deliver "all Moog non-public information in each Defendant's possession, custody or control" to a neutral vendor "if such information has been integrated or used by any Defendant in such a manner that such delivery necessarily includes property of any Defendant," by April 1, 2002. (*Id*., ¶ 2). In other words, devices that contain both Moog data and any Defendant's data would be turned over to the neutral vendor.

On April 1, Kim and Pilkington turned over a total of 23 devices to the neutral vendor, and Skyryse turned over Kim's Skyryse-issued laptop device, along with a hard drive containing

11,093 files pulled from Pilkington's Skyryse-issued laptop. (Andoh Dec., Exs. D, E). On April 29, over four weeks late (a violation of the March 11 Order), Skyryse turned over to the neutral vendor two additional laptops that were issued to Pilkington, and a thumb drive containing 568 additional files. (*Id*., Ex. G). On May 5, Skyryse belatedly turned over additional files to neutral vendor (a further violation of the March 11 Order). (*Id*., Ex. I).

C. Further Spoliation of Evidence and Violation of the March 11 Order

The March 11 Order also required the preservation of evidence. (*See* Dkt. 25, ¶ 5 (requiring that "Skyryse shall preserve and not otherwise tamper with or modify" its email, network drives, desktop computers, laptops, or other electronic devices"); ¶ 9 ("Each party shall preserve all evidence in that party's possession, custody, or control relevant to any party's claim or defense in this action, including electronically stored information"). However, between April 25 and 29, Skyryse disclosed to Moog and the Court that, among other things, multiple Skyryse employees had deleted evidence from devices. (*See, e.g.,* 4/26/22 Hrg. Tr. (ECF 95) at 18:17-18 ("[W]e have discovered forensically that since the complaint was filed certain information has been deleted.") & at 19:8-10 ("that is a fact on the ground as we sit here today, unfortunately, that the information was deleted after the complaint was filed"); Andoh Dec., Ex. H at p. 6 ("[S]ome employees appear to have deleted information from local computer drives after the litigation commenced."). Skyryse further disclosed to Moog that it had just imaged 37 of its devices for either containing evidence of such spoliation or evidence of Moog data, or both.

Though requested multiple times, Skyryse has thus far refused to provide basic details regarding the spoliation and Moog data discovered. (*See* Andoh Dec., Exs. F, H). For example, Skyryse failed to identify which Skyryse electronic devices contained evidence of deletions; or what specific items were deleted, the size and volume of any deletions, or when the deletions occurred. (*Id*., Ex. H). In response to Moog's inquiry about smartphones, Skyryse stated it "does

not issue smartphones to its employees," and disclaimed any obligations or responsibility for the personal devices that its employees use for work purposes (such as for sending and receiving Skyryse emails). (*Id*., pp. 1, 8). It is reasonable to assume, therefore, that Skyryse has not undertaken any efforts to preserve evidence on personal devices used for work purposes, meaning that evidence relevant to this case is likely being spoliated as we speak.

III. MOOG'S PROPOSED INSPECTION PROTOCOL SHOULD BE ADOPTED

A. Permitting Moog's Experts and Outside Counsel to Review the Forensic Images of the Devices Is Proper

As a general matter, it is proper for a defendant in a trade secret case to permit a plaintiff's experts and outside counsel to directly inspect forensic images of the defendant's devices, so long as the defendant is provided a reasonable opportunity to remove privileged documents. *See Allergan, Inc. v. Merz Pharms., LLC*, No. 11-cv-00446, 2011 WL 13323241, at *4 (C.D. Cal. June 9, 2011) (ordering in a trade secret misappropriation case that "Individual Defendants shall provide to Plaintiff forensic images of each of the media in question, subject to the opportunity of the Individual Defendants to eliminate any material for which a privilege or other objection to production is claimed"); *id.* at *3 (finding that the "balance [of interests] can best be achieved by allowing Plaintiff direct access to the forensic images of the media in question, consisting of hard drives and external storage media" and permitting defendants to "identify[] and excis[e] the objectionable material, together with creating a reasonably detailed log of those materials deleted and why"); *BalanceCXI, Inc. v. Int'l Consulting*, No. 19-CV-0767, 2020 WL 7034123, at *1–2 (W.D. Tex. Nov. 24, 2020) (ordering in a trade secret case that to the extent plaintiff "requests the laptop for examination in the future," plaintiff may employ a protocol whereby the "laptop [is] imaged" and plaintiff may conduct "examination of the Image"); *Physicians Interactive v. Lathian Sys., Inc.*, No. CA 03-1193-A, 2003 WL 23018270, at *10 (E.D. Va. Dec. 5, 2003) (ordering in

trade secret case that plaintiff is permitted to "enter the sites where the computers used in the alleged attacks are located and to obtain a 'mirror image' of the computer equipment containing electronic data relating to Defendants' alleged attacks on Physicians Interactive's file server"); *see also Audio Visual Innovations, Inc. v. Burgdolf*, No. 13-10372, 2014 WL 505565, at *3–4 (E.D. Mich. Feb. 3, 2014) (ordering in a trade secret case that forensic vendor provide list to both parties' counsel of all files on the device, including deleted files, that the defendant's counsel identify the files it seeks to excise for being objectionable in the form of a log, which the plaintiff's counsel has the right to challenge, and that *all other files* be produced to the plaintiff on a default AEO basis unless and until the parties confer on a different designation).

1. Privilege and Privacy Concerns Will Be Adequately Addressed

Moog's proposed protocol permits Defendants to review the forensic images of the devices for privileged documents and excise those prior to inspection, so long as a log is provided identifying the excised material. *See Allergan*, 2011 WL 13323241, at *4 ("For any such material eliminated, the Individual Defendants shall provide at the time of the production of the image in question a log identifying the eliminated material with reasonable particularity, along with a brief statement of the reason for eliminating it. The identification should contain, so far as reasonably possible, the identification of the location on the media of the eliminated material."). Moog does not expect the privileged material to be significant, as the devices turned over relate chiefly, if not entirely, to engineers, not lawyers. Pilkington and Kim in particular only worked for Skyryse for a brief period of time—from November 2021 and January 2022— prior to the devices being turned over, and almost every other former Moog employee who moved to Skyryse similarly did so in 2021 or 2022.[3] The vast majority of privileged documents will be readily identifiable, involving

[3] Out of 20 former Moog employees that moved to Skyryse, there are only three former Moog employees who moved to Skyryse prior to 2021.

a discrete group of lawyers (e.g., from the Gibson Dunn and Locke Lord law firms, for instance) and issues (e.g., pertaining to this lawsuit). Moreover, any burden from privilege review is reasonable for Defendants to bear. "Fundamental to this aspect of the law," i.e., privilege, is that "the party claiming the privilege has the burden of establishing and protecting it." *Allergan*, 2011 WL 13323241, at *2; *Id.* at *3 ("It is understood that [the privilege review] will be burdensome to the Individual Defendants. However, it is they who have interposed the objections. . . . [I]dentifying allegedly objectionable material[] [] should be the burden of the objecting party.").

Moog's proposed protocol also addresses concerns around personally private information on personal devices that were turned over by the individual defendants, permitting a privacy screen at the same time as the privilege screen. Consequently, the individual defendants do not object to Moog's proposed inspection protocol. (Andoh Dec., Ex. J, p. 2 (May 4, 2022 letter from individual defendants' counsel stating that the "personal privacy review [in Moog's proposed protocol] is sufficient to address the individual defendants' privacy concerns")).

2. The Inspection Would Be Subject to Heightened Security and Monitoring

Defendants have argued that Moog's experts and outside counsel should not be given "unfettered" access to the forensic images of the devices because they may contain Skyryse's trade secrets. But the access is anything but "unfettered." Moog's experts and outside counsel will not have physical possession of the devices or the forensic images of those devices—only the neutral vendor will. (*See* Andoh Dec., Ex. A, § III.A). The neutral vendor will host the forensic images on its own servers, called a "virtual machine" in Moog's proposed protocol. (*See Id.*, § III.B). Moog's experts and outside counsel will only be able to access the forensic images on the neutral vendor's virtual machine by using secure laptops (managed by the neutral vendor) in a secure environment. (*See Id.*, § III.D). The review of the forensic images by Moog's experts and outside counsel will also be monitored by the neutral vendor, including by videorecording. (*See Id.*, §

III.E). Finally, only Moog's outside counsel and experts will be able to access the forensic images. (*See Id.*, § VIII.B). The forensic images by default are designated "HIGHLY CONFIDENTIAL—OUTSIDE COUNSEL & EXPERTS' EYES ONLY," and Moog's outside counsel and experts are not permitted to disclose information from such designated material to in-house counsel or employees of Moog. (*See Id.*, § III.D.9).[4] Notably, only 5 of the 28 devices currently in the neutral vendor's possession were handed over by Skyryse, and Skyryse has given no indication that the remaining 23 devices belonging to Pilkington and Kim would contain Skyryse information.

To be clear, Moog's experts and outside counsel have no interest in Skyryse's so-called trade secrets. But they do need to inspect Skyryse's *documents* to investigate the extent to which they incorporate *Moog's* trade secrets from over 1.3 million files that Skyryse's employees have undisputedly stolen. That these Skyryse documents may incidentally contain Skyryse's so-called trade secrets is not sufficient reason to block Moog from conducting a full and fair investigation. It was Defendants who created this mess, and per the March 11 Order, the 28 devices they turned over necessarily contain Moog data.

3. Providing Access to Outside Counsel, in Addition to Experts, Is Appropriate and Necessary Here

Skyryse has argued that even if experts should get access to the forensic images, outside counsel should not. This argument makes no sense. Moog's outside counsel also need to be involved to provide input on the inspection, answer questions from the experts, and use the expert's work product in the context of the litigation. The experts are not lawyers, and cannot conduct an inspection in a vacuum without the assistance of outside counsel. The experts must be able to discuss their inspection work with outside counsel. Moreover, how particular material on the

[4] As noted in Moog's proposed protocol, however, to the extent a document is determined to not merit such a designation, Moog may request that Defendants produce the document under a less restrictive designation. (*See Id.*, § IV).

devices bears on the parties' legal claims and defenses is a legal question, and something that outside counsel will need to analyze and determine; to do so will require, in many instances, outside counsel to look at the material in question.

B. Skyryse's Proposed Protocol Would Be Improper and Insufficient Here

Skyryse's proposed protocol would only permit the neutral vendor to access the devices, and Moog would get no access. Moreover, the neutral vendor can only search for a "Moog Filename List," i.e., a list of the names of Moog files that were stolen, and a list of "hash values" corresponding to stolen files. (ECF 76-1, p. § III.3). The neutral vendor then searches for these file names and hash values and exercises its own "judgment" to determine whether the resulting hits contain Moog data (even though the neutral vendor has no expertise in either aviation software development or Moog data); Skyryse conducts a privilege screen on whatever the neutral vendor deems relevant; and then Moog gets whatever is left over. (*See id*., § III.6). In Skyryse's April 19, 2022 submission to the Court, Skyryse said it is willing to permit Moog to provide search terms (i.e., keywords), but only if Skyryse agrees to those terms. (ECF 76, p. 3). But the above approach is insufficient for reasons explained below.

1. Skyryse's Protocol Is Insufficient to Uncover Spoliation

Searching for keywords, Moog file names, and hash values would be insufficient to fully uncover the extent of the "alarming" spoliation that has occurred. Spoliation means a file has been deleted, resulting in the *absence* of a file and the *absence* of words that were once in that deleted file. While deleted files may be recoverable (i.e., not yet overwritten), such that a search for keywords might hit on those files, Skyryse has admitted that there is deleted data that is unrecoverable. (Apr. 26, 2022 Hrg. Tr. (ECF 95) at 19:5-6 ("[I]t also is the case that some of the information deleted may not be recoverable.") & 19:11 ("[W]e do not have certainty it will be recoverable.")). This is not surprising, as the theft here occurred months ago, long before the 28

devices were turned over to the neutral vendor in April and May. (*See* Bagnald Dec. (ECF 4-18), ¶¶ 8-10 (Kim theft occurring on November 19, 2021); Andoh Dec., Ex. C (Pilkington theft occurring on October 27 and November 12, 2021)). In fact, Skyryse has admitted to an additional 37 devices that they only *recently* imaged in late April. The likelihood of recoverable deleted data on those devices is very low.[5] Moreover, the personal devices of Skyryse employees that are used for work have apparently not been preserved at all, meaning that deletions may be occurring beyond recoverability as we speak.

2. Skyryse's Protocol Is Insufficient to Uncover Misappropriation

Searching for words, Moog file names, and hash values is insufficient to fully uncover Skyryse's misappropriation. As to words, many of the over 1.3 million stolen files are not chiefly composed of human words that can be searched. This would include drawings, designs, schematics, executables, images, models, diagrams, hand drawn figures, and object files, for example. Relatedly, much of the use is not literal copying at all, like copying an image from one device to another, but adapting Moog's processes, data flows, algorithms, structure, and architecture, where searching for words will be insufficient to find evidence of the use and theft. Searching for distinctive words is also completely ineffectual where these words were deliberately replaced to obfuscate the theft, or to adapt the material to Skyryse's existing systems.

As to Moog file names and hash values, these would only result in hits if Skyryse were to copy whole files, unaltered, onto its systems. But Moog expect this to constitute only a slim minority of the misappropriation here. *First*, a significant number of the stolen files contain Moog

[5] Skyryse has claimed that such imaging was merely prophylactic and that they cannot say with certainty that the deleted materials are relevant. But if they cannot and or will not provide details regarding what was deleted (and they have not, despite Moog having demanded this detail weeks ago), then that is precisely why Moog's outside counsel and experts should be granted direct access to inspect the forensic images. Neither Moog nor this Court should have to take Skyryse at its word that the deleted materials are of uncertain relevance.

proprietary statements, e.g., statements with headers like "MOOG PROPRIETARY AND CONFIDENTIAL INFORMATION." Moog does not expect Skyryse employees to copy a file wholesale because the inclusion of the Moog proprietary statement would make the theft too obvious. Another reason is that a whole file (as opposed to just portions of a file) may be more difficult to "plug" into the existing Skyryse projects or systems.

Instead, Moog suspects the vast majority of Skyryse's misappropriation to involve Skyryse employees treating Moog files as more of a "reference library" as they are developing Skyryse processes and products. For example, Skyryse employees are likely to pick and choose portions from the Moog "reference library" (e.g., a function here, a function there) to copy or incorporate into Skyryse documents, carefully excluding portions with the term "Moog" in them such as the Moog proprietary ownership statement, and replacing names and terms distinctive to Moog in order to obfuscate the theft.[6] Skyryse employees are also likely to use Moog files as a visual reference while they draft Skyryse documents—for example, using the same algorithms, structures, process flows, etc., but using different words to implement the foregoing (in order to, among other things, obfuscate the theft).

Notably, Moog does not even have accurate hash values to give to Skyryse, due to Defendants' own misconduct. For example, because Kim completely spoliated the external hard drive containing the 136,994 files she stole, those files are no longer in existence from which to generate hash values. Moog attempted to generate hash values from the files on Kim's Moog-issued laptop that *might* correspond to some of the 136,994 files, but that is largely impossible

[6] Using a litigation analogy, if someone were to plagiarize a brief, one would not expect that person to just pull the brief from PACER and then file it with the Court. The plagiarism would be too obvious, and the brief would not likely fit with the case. Instead, one would expect that person to pick and choose portions from the brief that he likes, discarding the rest, and incorporate the plagiarized portions into his own brief template and caption.

because Kim deleted 54 gigabytes of data from that laptop (corresponding to thousands of files) to cover up her copying and theft. Yet, Defendants seek to place the entire burden on Moog to identify hash values for the files *they* stole, without Moog having access to the most likely locations on which the files still exist (the 28 devices turned over), a classic Catch-22.[7]

3. Skyryse's Protocol Is Insufficient to Conduct a Forensic Analysis

Searching for keywords, Moog file names, and hash values is insufficient to conduct a forensic analysis of the 28 devices—e.g., an analysis of exactly when device A was connected to devices B, C, D, E, etc., what data was transferred from device A to devices B, C, D, E, etc. and vice versa; how data on these devices were accessed (whether viewed, edited, etc.); when data was deleted (spoliated) from those devices; and device history like date and time stamps, file access histories, file download histories, file upload histories, and so forth. *See Allergan*, 2011 WL 13323241, at *2 (finding that "the use of search terms to attempt to discover the suspected trails is awkward"). Only through direct inspection of the forensic images of the devices, including system files, can Moog's outside counsel and experts fully follow the trail of Defendants' misappropriation and spoliation. *See Allergan*, 2011 WL 13323241, at *2 ("[T]he interest of the

[7] On March 17, 2022, Skyryse's counsel sent an email saying, "To facilitate the procedures contemplated by the March 11, 2022 stipulation, we ask that Plaintiff promptly provide us with hash values, all file names, and any unique identifiers for each file Plaintiff alleges Defendants wrongfully acquired." In response, Moog referred Skyryse back to the log previously provided that showed the file paths, file names, and file sizes for all 136,994 files that Misook Kim had stolen, saying, "This information is sufficient for Defendants to comply with the March 11, 2022 stipulated order." Skyryse has used this to argue that granting Moog's experts and outside counsel access to the forensic images is unnecessary, because Moog admitted the log information was "sufficient." Not so, and Skyryse is clearly mischaracterizing Moog's statement. First, Moog was merely responding to Skyryse's request for identifiers of the stolen files—this discussion had nothing to do with the inspection protocol. Second, Moog was conveying that the log was "sufficient" information from ***Moog*** because Skyryse was required to expend some of its own effort to identify criteria to comply with the order; Skyryse was improperly trying to impose all the burden on Moog. Most importantly, Skyryse should have consulted with the individuals who stole the data, Mr. Pilkington and Ms. Kim, who are in the best position of anyone to know how to look for the information they stole.

Plaintiff in attempting to discover and then follow the trail (if it exists) of materials that allegedly have been unlawfully electronically transferred and/or deleted is very high."); *Gucci Am., Inc. v. Frontline Processing Corp.*, No. 09-cv-6925, 2010 WL 11655446, at *3 (S.D.N.Y. July 2, 2010) (where spoliation of evidence had occurred, ordering a forensic expert to image "the hard drives of computers owned by [various individuals] and provide the imaged drives to Plaintiff"); *Experience Hendrix, L.L.C. v. Pitsicalis*, No. 17-cv-1927, 2018 WL 6191039, at *2 (S.D.N.Y. Nov. 28, 2018) (circumstantial evidence of spoliation merited order that defendant produce forensic images directly to plaintiff of "every computing device physically located in the office(s) of—or otherwise associated with the business activities" of various parties); *Schreiber v. Friedman*, No. 15-cv-6861, 2017 WL 11508067, at *5 (E.D.N.Y. Aug. 15, 2017) (where "there is reason to believe that a litigant has tampered with the computer or hidden relevant materials that are the subject of court orders," ordering that forensic images of devices be made available to plaintiff's experts and outside counsel).

Moog's proposal is particularly appropriate where, as here, Skyryse's employees are alleged to have stolen Moog's data by transferring them onto the devices at issue. *See Id.* ("One factor contributing to the analysis is [that] it is a case involving departing employees who are alleged to have transferred protected date [sic] onto their personal storage media and also to have both deleted and further transferred it on."). Skyryse's employee, Kim, has also deliberately spoliated 136,994 files from an external hard drive and another 54 gigabytes of data from her Moog work laptop; and Skyryse has admitted to "alarming" deletions from other Skyryse employees. *See id.* (finding direct inspection of the device appropriate because "it is, at least in significant part, a case dealing with allegations of 'missing data' on the media in question").

4. Skyryse's Protocol Improperly Requires the Neutral Vendor to Identify Moog Confidential Information, Which It Lacks Expertise to Do

Skyryse's proposed protocol requires that even if keywords, Moog file names, or hash values hit on a document on the 28 devices, that that's not enough for a handover of that document to Moog. Instead, the neutral vendor must then "exercise independent judgment to determine whether a Target Document is likely to comprise or contain information confidential to Moog." (Andoh Dec., Ex. B, p. 3). This is unreasonable, and would be unacceptable even if running a search were sufficient to begin with (it is not), because the neutral vendor iDS lacks the expertise to exercise such judgment.

For example, to identify misappropriation of Moog's flight control software would require analyzing how Skyryse's flight control software is architected and the extent and nature of that architecture's similarities to Moog's, including by visually comparing code side-by-side where necessary. The reviewer must also know what the relevant flight control source code looks like, analyze Skyryse's repository logs to identify large check-ins of such source code, and exercise judgment based on experience to determine whether such check-ins are unusual and atypical in aviation software development. *See HP Tuners, LLC v. Cannata*, No. 18-CV-00527, 2020 WL 4905533, at *2 (D. Nev. Aug. 20, 2020) (ordering in trade secret misappropriation case that plaintiff's expert shell "be permitted to review, inspect and analyze[] . . . any and all firmware, software and source code (including all source control, changelogs and/or the history of all modifications to such firmware, software, and source code)" in the "mirror image of Defendant's Electronic Devices"). Unlike Moog's retained expert, iDS does not have expertise in flight control or aviation software development, and is not qualified to do this review. (*See* ECF 74-5 (information from iDS's website, showing that they do not identify as experts in aviation software development, or even software development generally)).

As another example, Defendants also stole Moog's repository of process assets, e.g., templates, checklists, tools, test cases, etc. pertaining to compliance with FAA regulations such as DO-178 and the related certification process. In fact, because Moog develops software at the highest level of criticality, much more time is spent on testing, reviews, and development of documentation that support the artifacts to show that the code complies with DO-178, than on the code itself. Moog has spent years developing the process assets for the DO-178 compliance approval and certification process. By stealing Moog's process assets, Skyryse is able to fast-track what would otherwise take it years to develop. To identify misappropriation of process assets requires someone with expertise in the DO-178 compliance and certification process. For example, the reviewer must analyze Skyryse's process for generating artifacts and whether it mimics Moog's artifacts; and compare the parties' templates, checklists, and other process assets for telltale similarities. To determine whether similarities between DO-178 process assets are unusual and likely the result of copying (rather than what you might typically find in process assets) requires the right experience and the execution of informed judgment. This is not a mechanical exercise.

Unlike Moog's retained expert, iDS does not have expertise in DO-178, FAA regulations governing software development, or related compliance procedures and certification. (*See* ECF 74-5). Nor should it, because that is not a set of qualifications that iDS was screened for; and it is outside the scope of the work iDS was retained to perform. Even in a more "ordinary" case of software theft—without all the process assets described above that are so specific to government regulations in the aviation industry—parties routinely rely on experts with specific source code and industry experience to conduct reviews and inspections. Here, iDS cannot fulfill the role necessary in order to uncover the misappropriation at the heart of this case.

What iDS does have adequate expertise to do is serve as an "escrow" agent for the devices and to forensically image those devices for Moog's inspection. This is why Moog intended for iDS to forensically image the devices and host those forensic images for inspection, and that iDS would host source code review for the case. Moog never proposed or agreed to iDS with the intent that they would serve in the role of reviewer of materials or "exercise judgment" as to what is Moog data. Indeed, none of the parties raised these capabilities with iDS during the vetting process and communications with iDS prior to engaging iDS on April 1. The Court's March 11 Order expressly leaves the details of who will conduct the inspection and how the inspection will be conducted unaddressed. (ECF 25, p. 3).

5. Skyryse's Protocol Would Cause Undue Delay

Skyryse's protocol would also inject needless and unacceptable delay into the discovery schedule, with far less effective results (which is perhaps Defendants' aim). It would make no sense for Moog to provide keywords, Moog file names, and hash values to the neutral vendor; have the neutral vendor take, say, a week to execute the search on 28 devices; have the neutral vendor take, say, another several weeks to "exercise its judgment" as to which contain evidence of misappropriation (even it had the expertise, which it does not); wait for Defendants to conduct their privilege review; then have Moog review the results and determine what further searches need to be conducted; and have the process start all over again, iteratively, *ad infinitum*. That is completely inefficient and would take too long and result in a massive and unnecessary prolongation of the expedited discovery schedule. Moog's experts know the case, know what to look for, and need to be able to conduct the inspection themselves, "following the trail" and adjusting their direction and process as they go along.

6. Producing Documents Is Not an Acceptable Substitute for Access to the Forensic Images

Skyryse has suggested that it might be willing to produce certain documents, like source code and process assets, to Moog for review, in lieu of granting Moog's experts and outside counsel access to the forensic images themselves. This is unacceptable for at least the following reasons:

First, Skyryse should already be producing source code, process assets, and other relevant documents, in response to Moog's document production requests, irrespective of the forensic images at issue. (*See* Andoh Dec., Ex. K, p. 9).

Second, while source code, technical documents, and process assets are certainly at issue, the full scope of the ways in which Defendants have misappropriated over 1.3 million files—covering a huge diversity of Moog's numerous projects, file types, and trade secrets—is unknown to Moog. Therefore, merely having Defendants produce certain types of information (like source code and process assets) is insufficient. At the very least, Moog's expert must be permitted to identify, through direct inspection of the forensic image of the devices, *what* has been stolen, copied, and integrated into Defendants' own documents, before Moog can craft comprehensive requests for production of specific categories of documents. Only Defendants fully know how they have misappropriated Moog's data and how they have integrated such data into their own documents. Moog should not be forced to "guess" at how they have misappropriated the data in order to provide search terms to Defendants while wearing a proverbial blindfold, but should instead be entitled to discover for itself the scope, depth, and breadth of Defendants' misappropriation. *Allergan*, 2011 WL 13323241, at *2 ("Another factor contributing to [the] analysis is the obvious fact that none of us knows what is actually contained on the sectors and fragments of the media involved. . . . Without mining through it, neither side really knows what is

out there. Matters of such potential importance should not be managed based upon suggestions or suspicions. Nor should they be approached with hit-and-miss methodology, if there is a reasonable alternative."). The source code and process assets, are just exemplary and only part of the picture.

Third, for Defendants to identify all source code, process assets, and other categories of documents across 28 devices will likely take an enormous amount of time—again, due to their apparent incapability or unwillingness to conduct a diligent search and identification, and the likelihood of this process fomenting multiplicative disputes requiring Court intervention. This will inject undue delay into the case and make it virtually impossible for the parties to comply with the expedited discovery schedule (which the parties have now had to revise twice already, including due to Skyryse's misconduct).

C. Defendants' Authorities Are Inapplicable and Distinguishable

The cases Skyryse relies on in its April 19 submission (ECF 76) are distinguishable on the law, facts, or both. Skyryse claims that forensic examinations of devices are "drastic" but relies on cases that do ***not*** involve trade secret claims. Cases involving claims of theft of trade secrets, however, are more likely to merit direct inspection by a plaintiff of forensic images of devices, especially where those devices contain the electronic materials that were stolen or misappropriated. *See Balboa Threadworks, Inc. v. Stucky*, No. 05-cv-1157, 2006 WL 763668, at *3 (D. Kan. Mar. 24, 2006) (distinguishing itself from trade secret cases, because "where trade secrets and electronic evidence are both involved, the Courts have granted permission to obtain mirror images of the computer equipment which may contain electronic data related to the alleged violation").

For example, Skyryse relies on *Aminov v. Berkshire Hathaway Guard Ins. Companies*, No. 21-CV-479-DG-SJB, 2022 WL 818944, at *1 (E.D.N.Y. Mar. 3, 2022), which involved insurance claims, not trade secret claims. The court found that a forensic examination was unwarranted because the request was "based on misplaced and unsupported speculation," *and* because "there is

no evidence of spoilation or alteration." *Id*. at *2. Likewise, *Popat v. Levy*, No. 15-CV-1052W(SR), 2021 WL 5166173 (W.D.N.Y. Nov. 5, 2021)—which involved discrimination and harassment claims, not trade secret claims—the court noted that "there is no reason to believe that plaintiff has tampered with the documents at issue in this matter." *Id*. at *2. Similarly, in *Calyon v. Mizuho Sec. USA Inc.*, 2007 WL 1468889 (S.D.N.Y. May 18, 2007), which also did not involve trade secret claims, the court specifically found that "[Plaintiff has not] argued that the Individual Defendants have made any representation that relevant documents or data have been lost, such that there may now be a need for [plaintiff] to conduct a more exhaustive electronic search in order to try to find that information. Nor has [plaintiff] identified any specific information that it seeks to recover from the mirror images, and shown that the Individual Defendants would not be capable of, or willing to, produce that particular information." *Id.* at *5. In *Wynmoor Cmty. Council, Inc. v. QBE Ins. Corp.*, 280 F.R.D. 681 (S.D. Fla. 2012), which involved a breach of an insurance contact, the defendants sought no forensic analysis regarding the devices (i.e., data regarding when devices were connected to other devices, what data was transferred on or off the devices, etc.), and there was no spoliation.

Here, by contrast to the cases above, the 28 devices are in the possession of the neutral vendor because they *presumptively* contain Moog data. There is also undisputed spoliation of nearly 137,000 files (Compl., ¶¶ 132, 137) and Skyryse has admitted that an additional 37 devices either have Moog data or evidence of deletion. Unlike in *Calyon*, Moog *has* identified specific information that it seeks to recover from the mirror images. (*See* Section III.B, *supra*.)

Skyryse also relies on *Sony BMG Music Ent. v. Arellanes*, No. 4:05-CV-328, 2006 WL 8201075 (E.D. Tex. Oct. 27, 2006), a copyright infringement case, the device at issue was the individual defendant's personal computer and she was concerned about guarding the privacy of

her personal information. Here, Skyryse's devices are not personal devices, and they have never claimed a personal privacy concern over its devices. (Indeed, they appear to have disclaimed all obligations—including preservation obligations—for personal devices of their employees). Meanwhile, the individual defendants, who did turn over personal devices, do not object to Moog's proposed protocol, noting that the "personal privacy review [in Moog's proposed protocol] is sufficient to address the individual defendants' privacy concerns." (Andoh Dec., Ex. J, p. 2).

As for cases involving trade secret claims: *Motorola Sols., Inc. v. Hytera Commc'ns Corp.*, 365 F. Supp. 3d 916 (N.D. Ill. 2019) is a trade secrets (and copyright infringement) case but the facts are completely distinguishable. There, the court found that the devices at issue were not relevant to the trade secret claims; that the request was untimely (requested weeks before the close of fact discovery); that the defendant had already produced "millions of pages" of evidence, making a forensic examination of the devices "overkill"; that the request for forensic examination was based on "mere skepticism and suspicion" that all relevant information has not been produced; and that the request was disproportional to the needs of the case because the devices were located in China and thus implicated "complex issues of Chinese law and state secrets." *Id*. at 923, 926, 927. Here, by contrast, the 28 devices are undisputedly relevant and not based on "suspicion" because the only reason Defendants turned them over to the neutral vendor is because they *presumptively* contain Moog data, pursuant to the March 11 Order. Defendants do not dispute that the devices require inspection—it is the mode of inspection that they dispute. Moog's demand for inspection was clearly timely, as it was made at the very outset of this case (and again, there was no dispute that inspection in concept was proper and indeed Defendants stipulated to this). Unlike in *Motorola*, Skyryse has produced a scant amount of documents to date, only about 150

documents (Moog meeting and conferring with Skyryse to remedy this failing). Finally, the devices here are all located in the U.S. and do not implicate foreign law.

Skyryse further relies on the inapposite cases *Ameriwood Indus., Inc. v. Liberman*, No. 06-CV-524, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006) and *Brocade Commc'ns Sys., Inc. v. A10 Networks, Inc.*, No. 10-cv-03428, 2012 WL 70428 (N.D. Cal. Jan. 9, 2012), which are trade secret cases, but neither of those cases involved the theft of over at least 1.3 million of the plaintiff's files (as has occurred here). *E.g., Brocade*, 2012 WL 70428, at *2 (disclosure of only 196 of plaintiff's files on the defendant's device). And neither of these cases involve a defendant who has indisputably spoliated nearly 137,000 stolen files and another defendant that has deleted further files on up to 37 devices (as has occurred here).

Skyryse relies on the above authorities to suggest that direct inspection of forensic images is not ordered in typical trade secret cases, but this is not correct. (*See* above & Section III.A, *supra*). But even if it were, the scale of theft, misappropriation, and spoliation that has occurred in this case is anything but typical.

IV. RELIEF REQUESTED AND CONCLUSION

Moog respectfully requests that the Court adopt and order Moog's proposed inspection protocol. Moog further requests that by May 19, 2022: (1) Skyryse complete its privilege review of the forensic images of its 5 devices currently in the neutral vendor's possession, such that the remainder of the forensic images (not containing privileged material) is made available for inspection to Moog's experts and outside counsel; and (2) provide its privilege log to Moog's outside counsel. Moog also requests that by June 2, 2022: (1) the individual defendants complete a privilege and privacy review of the forensic images of their 23 devices currently in the neutral vendor's possession, such that the remainder of the forensic images (not containing privileged and personally private material) is made available for inspection to Moog's experts and outside

counsel, on a rolling basis; and (2) provide their respective privilege and privacy logs to Moog's outside counsel, also on a rolling basis.

This dispute is ultimately about whether evidence at the heart of this case comes to light—or remains shrouded in secrecy, mystery, and obfuscation. Skyryse wants the latter. Moog submits that the former is proper, and is only achievable through an open, fair, and transparent inspection process, as requested above.

Dated: New York, New York
May 11, 2022

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
Attorneys for Moog Inc.

By: s/ Rena Andoh
Rena Andoh
Travis J. Anderson (*pro hac vice*)
Tyler E. Baker (*pro hac vice*)
Kazim A. Naqvi (*pro hac vice*)
30 Rockefeller Plaza
New York, New York 10112
212.653.8700

HODGSON RUSS LLP
Attorneys for Moog Inc.

By: s/Melissa N. Subjeck
Robert J. Fluskey, Jr.
Melissa N. Subjeck
Pauline T. Muto
The Guaranty Building
140 Pearl Street, Suite 100
Buffalo, NY 14202-4040
716.856.4000